Strategies for blocking traffic by a service or protocol

At some point you will want to block traffic based on the type of service or protocol that is being used. This is a fairly straightforward exercise if you are blocking all traffic using that service but it becomes subtler when trying to block it under specific circumstances or if you wish to block specific content in all circumstances. For the purposes of this explanation we will use FTP as an example, but the principles apply to many of the standard services.

Blocking all FTP traffic

In a policy, when the Service variable is set to a specific service and the firewall is set to DENY, what is happening is that it is blocking the port that is assigned to those Service names. In the case of FTP, FTP_GET, or FTP_PUT the firewall is blocking TCP port 21. Because you likely have some control over any FTP servers on your network this can be effective regarding incoming traffic but the situation changes when we start discussing outgoing traffic. If you could guarantee that all FTP traffic used the standard port then denying by service is an acceptable approach, but if someone has set up an FTP server out on the Internet that answers on a different port number, such as 60021, then denying traffic to the "FTP" service in the policy will not block the traffic. It will continue on to the next policy until finding one that applies to it, potentially finding a policy that has the service set to "ALL".

In the case of port number 60021 there are two approaches you could take. You could create a new service in the Firewall Objects section and assign the port number 60021 and deny by that. This only works if you know the port number being used out on the Internet. You could take the more effective approach and use an Application Control Profile to block all FTP traffic regardless of which port is being used.

Setting the UTM Proxy Option

Another thing that can be done to make the scanning of FTP more comprehensive than just looking for a specific port number is to edit the UTM Proxy Options. In the Protocol Port Mapping section of a profile the Inspection Port can be changed from a specific port to "Any" port. By doing this for the FTP protocol any traffic that is analyzed by a UTM Security Profile will check the traffic based on the FTP protocol not just the traffic going over the specific port currently assigned to FTP. Make sure that any policy that is analyzing with a UTM Profile uses a UTM Proxy Option profile that has FTP configured to inspect any port.

It is not just with FTP that you can do this. You can also set the FortiGate to check any port, not just the specified one, for the following protocols:

- HTTP
- SMTP
- POP3
- IMAP
- NNTP
- IM is already set to scan any port

Allowing FTP only to specific sites

One situation that does come up on a regular basis is the requirement for people of one organization to have the ability to use a specific FTP server out on the Internet, usually run by a partner organization. This can be allowed through the use of policies.

1. Obtain the IP address or FQDN of the approved FTP server.
2. From that address, create an address object in the Firewall Object section.
3. Make sure that existing policies do not allow FTP traffic to the other side of the FortiGate unit[1].
4. Create an Address policy that allows FTP traffic to the address created in Step 2 and place the policy early in the sequence before any policy that might DENY or block FTP.
5. Verify that it works.

Allowing FTP only for specified users

Any time you are referring to specific users you will likely end up using an Identity based policy. The two most common approaches to this are:

1. Those that can vs. those that can't
    i. Create a user group of those that is made up of users allowed to access FTP on the other side of the FortiGate unit.
    ii. Create a user group of those that is made up of users not allowed to access FTP on the other side of the FortiGate unit.
    iii. Make sure that existing policies do not allow FTP traffic to the other side of the FortiGate unit!.
    iv. Create a User Identity policy that allows traffic from the "allowed group" to go through the firewall and denies traffic from the "not allowed" group and place the policy early in the sequence before any policy that might DENY or block FTP.
    v. Verify that it works.

    The disadvantage of this approach is that it can require more administrative overhead to make sure that the correct users are in the correct group.

2. Those that can vs. everybody else
    i. Create a user group that includes the accounts of those users allowed to access FTP on the other side of the FortiGate unit.
    ii. Make sure that existing policies do not allow FTP traffic to the other side of the FortiGate unit!.
    iii. Create a User Identity policy that allows traffic from the "allowed group" to go through the firewall and place the policy early in the sequence before any policy that might DENY or block FTP.
    iv. Verify that it works.

    The advantage is that you only have to worry about the keeping the "allowed" users in the group. Everyone else is taken care of automatically.

Allowing FTP only for specified machines

Some organizations limit the use of some types of access to specific devices. If the organization uses static IP addresses then a regular Address policy can be used.

1. Using Address policies
    i. In the Firewall Objects section create address objects for any of the devices allowed to use FTP.

ii. Create an address group of addresses that make up devices allowed access.
iii. Make sure that existing policies do not allow FTP traffic to the other side of the FortiGate unit!.
v. Create a policy with the address group from Step ii. as a Source Address that allows the FTP traffic and place the policy early in the sequence before any policy that might DENY or block FTP.
iv. Verify that it works.

The disadvantage with this method is that if the addresses of the systems change the permissions will break down. The advantage is that it is simpler to set up.

2. Using Device Identity policies

This works almost exactly the same as allowing access by User Identity except that you would use a Device Identity policy instead of a User Identity policy.

i. In the User & Device section, define the devices that will be allowed to access FTP servers on the other side of the firewall.
ii. Add the devices from Step i. to a Device Group that is specifically for allowed FTP access.
iii. Make sure that existing policies do not allow FTP traffic to the other side of the FortiGate unit!.
vi. Create a Device Identity policy giving the group defined in Step ii the permission to use the FTP service to and place the policy early in the sequence before any policy that might DENY or block FTP.
iv. Verify that it works.

The advantage is that unless the network interface adapter hardware is changed on the computer you don't have to worry about changing addresses. This is handy in an environment where DHCP is used to assign addresses.

Allowing FTP except for specific content

If the objective is to block specific content from getting out but otherwise allow the use of FTP than the best approach is to use Data Leak Prevention (DLP). In this case it is very important to set the UTM Proxy Options to inspect any port. When the blocking of specific content is done, it is often done for legal or compliance reasons so you have to make sure

the content is blocked no matter which port it goes out on. If the content gets past the firewall there can be legal and/or financial consequences.

In setting up the DLP restriction, the assumption will be made that anyone can use FTP, it's just that they are not allow to send out certain confidential files.

1. Configure the UTM Proxy Option so that FTP scans any port.
2. Configure the DLP profile to scan for the content you wish to prevent leaving the network. You will be able choose from filtering options such as:
    - File size
    - Naming patterns using wild cards
    - Naming patterns using regular expressions
    - File types
    - File Finger Prints
    - Watermarks
    - Whether it is encrypted
3. Assign the action Block or Quarantine to the filters relating to the content.
4. Open any policy that the targeted content could go through, the closer to the beginning of the sequence the better.
5. Enable the use of the DLP profile that will block the content.
6. Make sure that the UTM profile referred to in Step 1 is chosen.
7. Include any other UTM details that are needed by the profile.
8. Verify that it works.

These strategies are not just for FTP. They can be used for a number of protocols that you may need to block selectively or pervasively. Also, these strategies were all fairly basic in their requirements. By combining the techniques listed here with each other or with other firewall techniques you can customize the restrictions imposed on your FortiGate to closely match your requirements.

[1] *The implicit policy or Policy 0 denies all traffic to all locations and this can be counted on to deny FTP traffic as long as there is not a policy before it that will allow the traffic.*